« La consommation énergétique annuelle du Bitcoin, équivalente à celle de la Suisse, pourrait être divisée par mille »

David Larousserie

Dans un entretien au « Monde », le mathématicien Jean-Paul Delahaye commente les avancées techniques récentes portées par Ethereum, concurrent du Bitcoin, qui pourraient renverser la hiérarchie des cryptomonnaies.

Jean-Paul Delahaye est professeur émérite de l'université de Lille, spécialiste d'informatique théorique et de la complexité des algo-rithmes. Il vient d'écrire ***Au-delà du bitcoin. Dans l'univers de la blockchain et des cryptomonnaies*** (Dunod, 270 pages, 19,90 euros), un livre pédagogique, mais aussi engagé, sur les forces et les faiblesses des cryptomonnaies, ainsi que sur leur avenir.

Publié le 24 septembre 2022 à 18h30

Pourquoi un mathématicien tel que vous s'intéresse-t-il aux cryptomonnaies ?

En 2008, Satoshi Nakamoto, dont on ignore toujours qui se cache derrière ce nom, a proposé un protocole, le Bitcoin, qui crée une monnaie indépendante de toute autorité centrale, dont le fonctionnement repose sur un contrôle collectif, le tout étant robuste et sûr. L'idée-clé est celle de la blockchain, une sorte de livre de comptes enregistrant les transactions sans possibilité d'effacer des pages, qui est partagé dans tout le réseau. C'est une invention géniale. Avant lui, d'autres avaient essayé de développer des monnaies électroniques, mais sans succès. Ce qui est neuf et révolutionnaire est la mise au point d'un protocole qui assemble des fonctions déjà connues, mais d'une façon inattendue, et que personne n'avait imaginée.

Ce protocole a, de plus, bénéficié de plusieurs avancées pour se lancer en 2009. Le chiffrement, essentiel au fonctionnement, était assez mûr, comme le montre le succès des transactions bancaires sur Internet. De même, les réseaux pair à pair ou distribués fonctionnaient depuis plusieurs années sans problème. Enfin, comme le système re- pose sur le partage d'un gros fichier d'environ 500 Go, il fallait que les ordinateurs aient assez de mémoire et de capacité de calcul.

Pourtant, vous prévoyez l'échec de Bitcoin, que vous qualifiez de « diplodocus », de « Minitel des cryptomonnaies », à « ranger dans un musée de l'informatique ». Pourquoi ?

Le problème principal du protocole réside dans la manière dont sont désignés les validateurs des nouvelles pages de transactions à enregistrer dans la blockchain. Avec Bitcoin, le validateur choisi est celui qui remporte un concours de calcul équivalant à proposer une sorte de grille de Sudoku valide de plus en plus grande, ou sortir un sextuple six avec six dés... En pratique, le calcul est lié à un problème cryptographique difficile. La conséquence est qu'il y a une compétition, de plus en plus dure et de plus en plus coûteuse en énergie. Au départ, la dépense énergétique était faible, puis elle a décuplé environ tous les ans pour représenter, selon les estimations, l'équivalent de la consommation annuelle de la Suisse ou de la Suède, de l'ordre de 100 térawattheures ! Or c'est une dépense inutile, car on peut se passer de ce type de méthode. C'est pour cela que je parle de bug, d'erreur pour Bitcoin, qui aurait pu être mieux conçu dès le départ.

Mais comment faire autrement ?

C'est ce que vient de faire une autre blockchain, Ethereum, le 15 septembre. Deuxième au monde derrière Bitcoin en termes de capitalisation, elle utilisait depuis sa création, en 2015, la même méthode dite « de preuve de travail », et vient de passer à une autre méthode dite « de preuve d'enjeu ». Cette fois, les validateurs ont une probabilité d'être sélectionnés qui dépend de la quantité d'argent qu'ils mettent en dépôt, et qu'ils récupéreront quand ils se re- tireront du « jeu ». Pour cela, aucune dépense superflue d'énergie n'est nécessaire ; seules les quelques centaines d'ordinateurs formant le réseau suffisent. Les validateurs sont rémunérés en recevant de nouvelles unités de compte. Sur le plan de la sécurité, il n'y a pas vraiment de différence entre les preuves de travail et d'enjeu. D'ailleurs, des réseaux comme Cardano et Solana, qui utilisent des preuves d'enjeu depuis des années, gèrent des milliards d'euros en circulation et n'ont pas été attaqués.

Les créateurs d'Ethereum estiment que la consommation électrique sera divisée par environ 200 avec ce changement de méthode. Si Bitcoin le faisait, la con- sommation serait réduite de mille ou plus.

Pourquoi Bitcoin n'adopte-t-il pas cette solution ?

Il y a plusieurs obstacles. Le premier, inavouable pour ses défenseurs, est que cela pourrait faire baisser les cours du bitcoin et donc leurs intérêts. Le second est que cela fera perdre de l'argent à ceux qu'on appelle les « mineurs », c'est-à-dire ceux qui font ces calculs coûteux et absurdes et en retirent une rémunération. Ils ont dû investir dans des ordinateurs qui deviendraient inutiles.

Depuis le changement opéré par Ethereum, j'observe déjà que des entre- prises de minage ferment ou que d'autres vendent leur matériel. Mais ce ne sont pas les mêmes dispositifs de cal- cul qui sont utilisés : d'un côté des cartes graphiques (Ethereum), de l'autre des circuits intégrés dédiés (ASIC). Cer- tains mineurs se rabattent vers une ancienne branche d'Ethereum, mais je ne leur prédis pas une grande réussite, car la valeur de cette cryptomonnaie, Ethereum classic, est faible.

Enfin, le dernier obstacle est lié à la gouvernance de ces systèmes collectifs, qui passe par des votes, où les mineurs ont le plus de poids. Ethereum a mis cinq ans à faire cette transformation et a bénéficié de l'appui des plates-formes d'échanges de cryptomonnaies qui ont soutenu l'initiative. Cette dernière a quand même été un exploit technique, comparable, selon certains, à changer le moteur d'un avion en plein vol. Des milliards d'euros étaient en jeu et jusqu'à présent ça marche.

Le cours de l'ether a pourtant baissé ?

Il y a eu une baisse, mais elle semble s'être arrêtée. Certains notent que c'est plutôt la hausse avant le changement qui est significative, puisque l'ether valait 0,052 bitcoin il y a trois mois et 0,07 aujourd'hui. Il se peut aussi que les défenseurs acharnés du bitcoin, qui ne veulent pas qu'on puisse dire que le changement va conduire à un renversement entre Bitcoin et Ethereum, vendent des ethers et soutiennent le bitcoin. Je reste persuadé qu'à moyen terme, la capitalisation des ethers passera au- dessus de celle des bitcoins. Au- jourd'hui, dans la capitalisation totale des cryptoactifs, les bitcoins représentent 39 % et les ethers 18 %.

D’autant que, vous le rappelez dans le livre, Ethereum, comme d’autres blockchains, hormis Bitcoin, a d’autres atouts, notamment grâce aux « smart contracts », qui attirent beaucoup de monde. Qu’est-ce que c’est ?

Je prédis un grand avenir à cette autre innovation apportée par Ethereum dès son lancement. Il s’agit de programmes informatiques qui tournent sur le réseau et dont le bon fonctionnement est vérifié grâce au réseau de validateurs de la blockchain principale. Le fournisseur du logiciel n’en a plus le contrôle centralisé et son code source est ouvert. L’intérêt est de développer de nouvelles applications en profitant d’une infrastructure de confiance. L’une des premières applications a été de créer de nouvelles cryptomonnaies sur la base d’Ethereum. On en a ainsi des milliers, qui bénéficient du même réseau de validateurs. En out- re, pour les financer, des levées de fonds dites initial coin offering (ICO), ont pu être organisées et validées grâce à ces smart contracts d’Ethereum.

Ces programmes peuvent aussi créer des jeux, comme des loteries. Ou bien des « jetons stables », dont la valeur ne change pas et qui offrent de la fluidité monétaire. Ou alors des jetons non fongibles, les NFT, qui affolent le marché de l’art en ce moment, qui sont des sortes de produits dérivés d’une œuvre à l’unicité garantie. Ces smart contracts sont vraiment un progrès extraordinaire, qui rend le protocole plus complexe, mais qui apporte d’autres fonctionnal- ités.

Quelles sont les faiblesses des cryp- tomonnaies ?

Ces technologies reposent sur des pro- grammes informatiques, qui peuvent donc être sujets à des bugs, des failles. Bitcoin a eu à en subir en 2010, ce qui avait permis à un hackeur de générer 184 milliards de faux bitcoins, alors que leur nombre est plafonné à 21 millions. Cela a pu être corrigé.

Ces réseaux peuvent également être at- taqués. Il « suffit », en principe, qu’un attaquant contrôle 51 % des pages ajoutées à la blockchain et ce risque ex- iste aussi bien pour les preuves d’enjeu que de travail. La littérature scientifique est remplie aussi d’attaques, plus théoriques que réalistes. Enfin, la sécu- rité repose sur la robustesse de fonctions cryptographiques, dont on ne dispose pas de la preuve mathématique qu’elles sont inviolables.

Quels scénarios prévoyez-vous ?

Dans le livre, j’explore quatre scénarios principaux qui reposent en grande partie sur l’avenir de Bitcoin lui-même : autodestruction, interdiction, cohabitation ou « victoire ». Comme je l’ai dit, je ne crois pas que Bitcoin survivra longtemps à cause du coût énergétique. Mais il peut aussi s’effondrer à cause d’un bug, d’une rupture de confiance... L’interdiction est possible aussi car les États ne se laisseront pas faire et n’abandonneront pas facilement l’instrument de politique économique que constituent les monnaies. Ils pourraient aussi légiférer pour empêcher toutes sortes de trafics ou d’escroqueries permis par l’anonymat de certaines blockchains. La cohabitation est peut-être le plus probable : des cryptomonnaies, mais probablement pas le bitcoin, coexisteraient avec les monnaies centrales. Enfin, certains rêvent de l’abandon des monnaies centrales, comme les fondateurs et les promoteurs de Bitcoin le souhaitaient, mais un nouvel ordre mondial monétaire serait alors à construire.